Crittografia al liceo: approfondire le classi di resto modulo n

Crittografia al liceo: approfondire le classi di resto modulo *n*

Ottavio G. Rizzo[1], Emanuele Cesena[2]
[1]*Dip. di Matematica, Università degli Studi di Milano*
Via Saldini 50, 20133 Milano (MI)
ottavio.rizzo@unimi.it
[2]*Dip. di Automatica e Informatica, Politecnico di Torino*
Corso Duca degli Abruzzi 24, 10129 Torino (TO)
emanuele.cesena@polito.it

In questo lavoro presentiamo una proposta didattica per approfondire le classi di resto modulo n attraverso un percorso nella storia della crittografia. Dal cifrario di Cesare al moderno schema RSA, passando attraverso i classici per sostituzione e Vigenère, abbiamo organizzato un ciclo di laboratori didattici tenuto presso alcuni licei di Milano. Il materiale didattico è disponibile all'indirizzo www.mat.unimi.it/users/labls/Crittografia.

1. Introduzione

La tradizionale didattica della matematica, che privilegia ascolto passivo ed attività talvolta meccaniche e ripetitive, porta generalmente a scarsa motivazione da parte degli alunni e ad un apprendimento volatile e povero di spessore. Attraverso un approccio meno formale, è possibile sviluppare temi specifici e conseguire risultati significativi in direzione del controllo consapevole delle nozioni e dei concetti appresi.

Il laboratorio di crittografia oggetto di questo articolo è stato svolto in seno al Progetto Lauree Scientifiche, organizzato dal Dip. di Matematica dell'Università degli Studi di Milano ed inquadrato nell'ambito dello schema del progetto nazionale "Orientamento e formazione degli insegnanti – matematica". Il progetto (di durata biennale: 2005–2007) si proponeva di portare gli studenti insieme ai loro insegnanti a fare qualche **esperienza di matematica** su alcuni temi stimolanti e significativi, attraverso l'istituzione di laboratori didattici della durata complessiva di 8 ore.

In questo lavoro, proponiamo un percorso nella storia della crittografia a partire dalle origini fino ai sistemi moderni, utilizzati realmente ad esempio nelle comunicazioni sicure via Internet (non sottovalutiamo l'importanza per un adolescente di realizzare che i concetti astratti presentati a lezione trovano riscontro nella propria vita quotidiana). La storia della crittografia, con il suo alternarsi di nuove idee per crittosistemi ed attacchi agli stessi, ha un'innegabile attrattiva che catalizza l'attenzione verso il problema matematico. Nel nostro percorso abbiamo voluto stabilire un parallelo tra la crittografia e le proprietà di $\mathbf{Z}_n$, l'insieme delle classi di resto modulo n: sfruttando il fascino della

DIDAMATICA 2011 – ISBN 9788890540622

crittografia, possiamo introdurre concetti algebrici come anelli e campi e descrivere problemi di natura più algoritmica come il problema della fattorizzazione o il calcolo delle potenze modulo *n*.

2. Cifrario di Cesare: la somma in Z_n

La nostra storia della crittografia è accompagnata da **Codici e Segreti** [Singh, 2001], un bel saggio che proponiamo come lettura sia agli insegnanti che agli studenti.

Il primo esempio che presentiamo è il famoso cifrario di Cesare, che Svetonio descrive così: *si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet* [Suetonius].

La relazione con la somma in $\mathbf{Z}_n$ è evidente: codifichiamo ciascuna lettera dell'alfabeto come un elemento di $\mathbf{Z}_{26}$ (A = 1, B = 2, ...) ed indichiamo con *m* una lettera del messaggio in chiaro e con *c* la corrispondente nel messaggio cifrato; scelta una chiave $k \in \mathbf{Z}_{26}$, per cifrare e decifrare si operano le seguenti trasformazioni:

$$c = m + k \pmod{26} \qquad m = c - k \pmod{26}$$

(nel caso descritto da Svetonio la chiave è k=3, infatti per decifrare occorre sottrarre 3).

Tanto semplice è il cifrario, tanto semplice è romperlo. Poiché il cifrario di Cesare si limita a **traslare** tutte le lettere di una stessa ampiezza, si tratta semplicemente di trovarla. In realtà, essendoci solo 26 chiavi, potremmo anche limitarci a provarle tutte e 26 finché non otteniamo un testo sensato, ma questo metodo non è molto istruttivo... Più interessante è invece sfruttare l'analisi di frequenza: la distribuzione delle lettere nell'italiano standard (mostrata in Fig.1, sinistra) ha tre picchi ravvicinati: A, E ed I, quest'ultimo seguito dai due "buchi" della J e della K. Calcolando la frequenza delle lettere nel testo cifrato, ci aspettiamo di trovare un profilo analogo, ma traslato (come ad esempio in Fig.1, destra). La chiave corrisponde, come già osservato, all'ampiezza della traslazione.

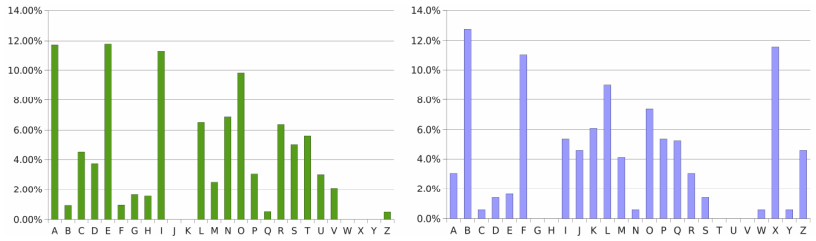

Fig.1 – (Sinistra) Distribuzione di frequenza delle lettere nell'italiano standard, fonte [Singh, 2001]. (Destra) Distribuzione in un brano tratto dalle *Ultime lettere di Jacopo Ortis* di Ugo Foscolo, cifrato con Cesare con chiave *k*=-3 (il picco della A a sinistra è traslato sul picco della X a destra).

3. Cifrari per sostituzione e di Vigenère

Nella seconda lezione presentiamo esempi decisamente più significativi: il cifrario per sostituzione (sostituzione semplice), la sua crittoanalisi (sempre basata sull'analisi di frequenza, questa volta un po' più raffinata rispetto al cifrario di Cesare) e il cifrario di Vigenère. La crittoanalisi di Vigenère è rimandata alla terza lezione, lasciando agli studenti il piacere di confrontarsi con il metodo che, ritenuto inattaccabile per secoli, si è conquistato la fama di **chiffre indéchiffrable**. Come curiosità didattica, segnaliamo che un paio di studenti si sono addirittura cimentati in un attacco a forza bruta al computer… sfortunatamente senza successo per errori di implementazione.

Entrambi i cifrari non hanno una relazione diretta con le proprietà di $\mathbf{Z}_n$ che ci interessa discutere in questo lavoro, pertanto ne omettiamo ulteriori dettagli.

4. Cifrario per affinità: proprietà di anello di $\mathbf{Z}_n$

Nella terza lezione, oltre alla crittoanalisi di Vigenère, iniziamo a porre le basi per la discussione del problema fondamentale della crittografia: la gestione delle chiavi.

Se in Cesare scambiarsi una chiave corrispondeva a scambiarsi un elemento di $\mathbf{Z}_{26}$, nel cifrario per sostituzione la chiave è ben più grande ed occorre scambiarsi un intero alfabeto ossia, senza stare a fare troppo i raffinati, 26 elementi. Con il cifrario per affinità possiamo realizzare uno schema che assomiglia molto ad un cifrario per sostituzione (nel senso che l'alfabeto per la sostituzione è "abbastanza" casuale), senza tuttavia doverci scambiare un intero alfabeto, ma solo 2 elementi.

Nel cifrario per affinità, la chiave sono due elementi a, $b \in \mathbf{Z}_{26}$, di cui a invertibile, cioè esiste un elemento $a^{-1} \in \mathbf{Z}_{26}$ tale che $a \cdot a^{-1} \equiv 1 \pmod{26}$. Per cifrare e decifrare calcoliamo:

$$c = a \cdot m + b \pmod{26} \qquad m = (c - b) \cdot a^{-1} \pmod{26} .$$

Il cifrario per affinità è lo spunto per una serie di interessanti discussioni. In primis la moltiplicazione in $\mathbf{Z}_n$ e quindi le proprietà di anello. Importante è anche l'esistenza dell'inverso di a, necessaria per la decifratura: come è noto, in $\mathbf{Z}_n$ sono invertibili solo gli elementi coprimi con n, che sono in numero di $\varphi(n)$. Volendo, questo discorso può essere ampliato notando che se n è primo, allora tutti gli elementi non nulli sono invertibili e questo ci porta alla nozione di campo. Oppure, chi preferisse questioni geometriche, può soffermarsi sul passaggio da Cesare, traslazione, a questo cifrario per affinità, in cui possiamo facilmente individuare l'omotetia (moltiplicazione per a – invertibile!) e la traslazione (somma di b).

È da notare che il cifrario per affinità non ha un grande valore dal punto di vista crittografico: è un cifrario per sostituzione, quindi attaccabile con l'analisi di frequenza. Diciamo, per essere onesti, che il cifrario per affinità non è che una scusa per dirigere l'attenzione degli studenti verso le nozioni matematiche.

5. Crittografia Moderna e RSA: potenze in Z_n

L'ultima lezione è incentrata sulla crittografia a chiave pubblica e più in generale sulla crittografia moderna.

La **crittografia a chiave pubblica** nasce alla fine degli anni '70 per rispondere ad una precisa esigenza: scambiarsi delle chiavi crittografiche su un canale insicuro. La rivoluzione della crittografia a chiave pubblica consiste nel disaccoppiare la chiave di cifratura (che può essere pubblica), da quella di decifratura (che deve necessariamente rimanere privata).

Il primo schema di cifratura a chiave pubblica è stato RSA [Rivest et al, 1978], che prende il nome dai suoi inventori: Rivest, Shamir ed Adleman. RSA è basato sul problema della fattorizzazione, è tuttora inviolato ed utilizzato nella maggior parte delle comunicazioni protette via Internet.

Per utilizzare RSA dobbiamo innanzitutto costruire una coppia di chiavi pubblica e privata: si scelgono due numeri primi (grandi) p e q e si calcola il prodotto $n = p \cdot q$; si sceglie quindi un intero e, invertibile modulo $\varphi(n)$, e si calcola $d = e^{-1} \bmod \varphi(n)$. La chiave pubblica è la coppia (e, n), mentre la chiave privata è (d, n). La chiave pubblica può essere distribuita e sarà utilizzata da tutti coloro che vogliono cifrare un messaggio. La chiave privata rimane segreta e sarà utilizzata per decifrare i messaggi ricevuti. Per cifrare e decifrare messaggi, si calcolano:

$$c = m^e \pmod n \qquad\qquad m = c^d \pmod n \ .$$

Tralasciando, per ragioni di spazio, il perché RSA funziona – una semplice verifica sfruttando il piccolo teorema di Fermat – osserviamo invece che per rompere RSA occorre calcolare d, ossia invertire e mod $\varphi(n)$; questo richiede calcolare $\varphi(n) = (p - 1) \cdot (q - 1)$ (p e q sono primi), che è equivalente a fattorizzare n. Quando n è sufficientemente grande, dell'ordine di 2^{1024}, questo problema è intrattabile.

Per ulteriori dettagli, ad esempio il calcolo delle potenze modulo n, rimandiamo al materiale didattico disponibile all'indirizzo: www.mat.unimi.it/users/labls/Crittografia.

Bibliografia

[Singh, 2001] Singh S., Codici & Segreti (The Code Book), BUR Biblioteca Univ. Rizzoli, Milano, 2001.

[Wikipedia] Wikipedia, the free encyclopedia. Contiene, sia in italiano che in inglese, approfondimenti per tutti i cifrari menzionati (Cesare, sostituzione, Vigenère, RSA). www.wikipedia.org.

[Suetonius] Suetonius Tranquillus G., De vita Cæsarum, dal Libro 1, Capitolo LVI.

[Rivest et al, 1978] Rivest R. L., Shamir A., Adleman L., A method for obtaining digital signature and public key cryptosystems. Communications of the ACM, 21, 1978, 120-126.